SEJA CIBERESPERTO
#CyberMonth

MÊS DA CONSCIENTIZAÇÃO EM CIBERSEGURANÇA 2021: FAÇA SUA PARTE. #BECYBERSMART

CIBERSEGURANÇA NO TRABALHO

As empresas sofrem grandes perdas financeiras quando ocorre um ataque cibernético. Em 2020, houve um aumento acentuado nos ciberataques que atingem empresas usando logins e senhas roubados.[1] Cibercriminosos frequentemente contam com uma falha humana — funcionários que não instalam patches de software ou clicam em links maliciosos — para ganhar acesso ao sistema. Desde a alta administração até os funcionários recém-contratados, a cibersegurança requer que todos estejam vigilantes para manter dados, clientes e o capital seguros e protegidos. Seja ciberesperto (#BeCyberSmart) para se conectar com confiança e contribuir para uma cultura de cibersegurança na sua organização.

DICAS SIMPLES

- **Trate as informações da empresa como informações pessoais.** As informações da empresa geralmente incluem uma mistura de dados pessoais e sigilosos. Talvez você esteja pensando em segredos industriais e nas contas de crédito da empresa, mas isso também inclui as informações de identificação pessoal (PII, do inglês personally identifiable information) dos funcionários contidas em formulários do imposto de renda e folhas de pagamentos. Não compartilhe PII com desconhecidos ou usando redes desprotegidas.
- **Não deixe que as senhas sejam fáceis de adivinhar.** À medida que a tecnologia "inteligente" ou direcionada pelos dados evolui, é importante lembrar que as medidas de segurança só funcionam se forem utilizadas corretamente pelos funcionários. A tecnologia inteligente é movida a dados, o que significa que dispositivos como smartphones, laptops e impressoras sem fio, entre outros, estão constantemente trocando dados para realizar tarefas. Tome as precauções adequadas de segurança e assegure que os dispositivos sem fio tenham a configuração correta para evitar violações de dados. Para mais informações sobre a tecnologia inteligente, consulte Dicas sobre a Internet das Coisas.
- **Mantenha tudo atualizado.** Mantenha seu software atualizado na última versão disponível. Faça suas configurações de segurança para manter suas informações seguras, habilitando atualizações automáticas para não precisar pensar nisso, e configure o software de segurança para fazer varreduras regulares.
- **As redes sociais fazem parte das ferramentas contra fraude.** Por meio de uma busca no Google e uma varredura nos sites da sua organização nas redes sociais, os cibercriminosos podem recolher informações sobre seus parceiros e fornecedores e sobre os departamentos de recursos humanos e financeiro. Os funcionários devem evitar a indiscrição nas redes sociais e não devem conduzir negócios oficiais, enviar ou receber pagamentos nem compartilhar PII em plataformas de redes sociais. Leia Dicas de cibersegurança em redes sociais para obter mais informações.
- **Basta uma vez.** É incomum que ocorram violações de dados quando um cibercriminoso hackeia a infraestrutura de uma organização. Muitas violações de dados podem ter sua origem atribuída a uma única vulnerabilidade de segurança, tentativa de phishing ou evento de exposição acidental. Desconfie de remetentes atípicos, não clique

em links desconhecidos e apague mensagens suspeitas após notificar ou encaminhar todas as tentativas de phishing para um supervisor, de forma que se possa implementar qualquer atualização, alerta ou mudança no âmbito da organização. Para mais informações sobre fraudes por e-mail e phishing, Leia Dicas sobre phishing.

SE VOCÊ TRABALHA EM CASA

- **Use apenas as ferramentas aprovadas.** Use apenas software e ferramentas aprovados pela organização para o trabalho, incluindo ferramentas de videoconferência e de colaboração fornecidas ou aprovadas pela empresa para iniciar e marcar reuniões.
- **Proteja sua reunião.** Personalize as precauções de segurança para que sejam adequadas ao público pretendido. Tenha um plano sobre o que fazer se uma reunião pública for interrompida. Tome precauções para garantir que só os indivíduos esperados participem da reunião.
- **Proteja suas informações.** Personalize suas precauções de segurança conforme o grau de sigilo dos seus dados. Compartilhe somente os dados necessários para atingir as metas da sua reunião.
- **Proteja-se.** Tome precauções para não revelar acidentalmente informações. Assegure-se de que as redes domésticas estejam protegidas. Para mais informações, acesse Materiais de referência sobre teletrabalho para funcionários em casa.

ENTRE EM CONTATO COM A EQUIPE DO MÊS DA CONSCIENTIZAÇÃO EM CIBERSEGURANÇA DA CISA

Agradecemos o seu contínuo apoio e compromisso com o Mês da Conscientização em Cibersegurança e sua ajuda para manter todos os americanos seguros e protegidos on-line. Envie um e-mail para nossa equipe no endereço CyberAwareness@cisa.dhs.gov ou acesse www.cisa.gov/cybersecurity-awareness-month ou https://staysafeonline.org/cybersecurity-awareness-month/ para saber mais.

RECURSOS

1. Centro de Recursos de Roubo de Identidade. (2021). *Relatório sobre violações de dados de 2020* https://www.idtheftcenter.org/annual-reports/